

## REMARKS

Applicant has carefully studied the outstanding Official Action. The present amendment is intended to be fully responsive to all points of rejection and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the present application are hereby respectfully requested.

The specification stands objected to because the title of the invention is missing at the top of the first page of the specification. The specification has been amended to add the title.

Claims 1 - 11, 14, and 15 stand rejected under 35 USC 103(a) as being unpatentable over US Patent 5,987,134 to Shin et al in view of US Patent RE 37,178 to Kingdon, and further in view of US Patent 6,377,691 to Swift et al.

Shin et al describes a device and method for authenticating a user's access rights to resources, including a challenge - response and proof mechanism.

Kingdon describes a method and apparatus for authentication of client-server communication, which is intended to prevent the forging of message packets.

Swift et al describes a challenge-response authentication protocol intended for use with datagram-based remote procedure calls.

The present invention, as claimed in claim 1, comprises a method for verifying that a prover has access to a private key associated with a public key. The recitation of claim 1 includes the following (emphasis added): "the verifier choosing a challenge Q and a padding string X; the verifier sending an initialization message to the prover, the initialization message comprising a disguised form Y produced by applying a public disguising function Fp to Q and X, Y being equal to Fp(Q,X); ... the prover verifying that Y=Fp(Q,X)".

Applicant respectfully points out that, in rejecting claim 1, the Examiner did not refer to the portion of the recitation of claim 1 emphasized above. Therefore, the Examiner failed to make a *prima facie* case that claim 1 is unpatentable. The Examiner's rejection of claim 1 should therefore be withdrawn.

Furthermore, Applicant has carefully studied Shin et al, Kingdon, and Swift et al and finds that the indicated features of claim 1 are neither described nor suggested in any of the references cited by the Examiner.

Claim 1 is therefore deemed allowable.

Claims 2 - 11 depend directly or indirectly from amended claim 1 and are therefore deemed allowable.

Claim 14 is a system claim corresponding to method claim 1 and is deemed allowable with reference to the above discussion of the allowability of claim 1.

Claim 15 is an apparatus claim corresponding to method claim 1 and is deemed allowable with reference to the above discussion of the allowability of claim 1.

Claim 12 stands rejected under 35 USC 103(a) as being unpatentable over Shin et al in view of Swift.

Claim 13 stands rejected under 35 USC 103(a) as being unpatentable over Shin et al in view of Swift, and further in view of US Patent 6,434,238 to Chaum et al.

Chaum et al describes a multi-purpose transaction card system in which cards make use of a variety of cryptographic confidentiality and authentication methods.

Claims 12 and 13 have been cancelled without prejudice. Discussion of the rejection of claims 12 and 13 is therefore deemed to be unnecessary.

Applicant has carefully studied the other prior art of record including:

US Patent 6,073,234 to Kigo et al, which describes a device for authenticating user's access rights using authentication and proof techniques;

US Patent 6,516,413 to Aratani et al, which describes an apparatus and methods for user authentication using verification and proof techniques;

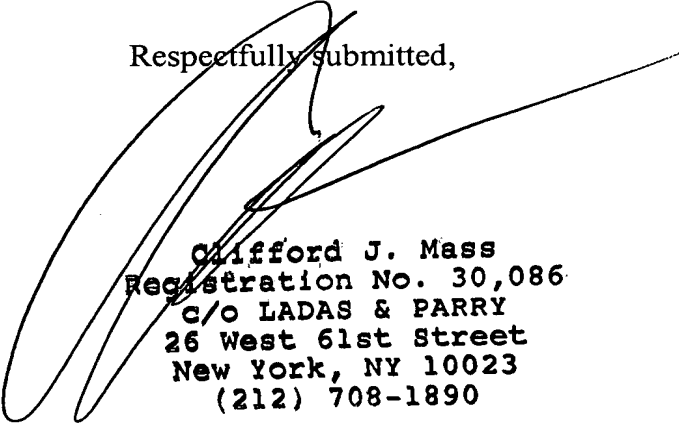
US Published Patent Application 2001/0005899 of Tanaka, which describes a method and system for controlling usage of a simulator, including random setting of a simulation condition; and

US Patent 6,353,888 to Kakehi et al, which describes access rights authentication apparatus using authentication and proof techniques.

Applicant finds that the present invention as claimed is neither described nor suggested in the prior art of record, taken either individually or in combination.

In view of the foregoing remarks, it is respectfully submitted that the present application is now in condition for allowance. Favorable reconsideration and allowance of the present application are respectfully requested.

Respectfully submitted,



Clifford J. Mass  
Registration No. 30,086  
c/o LADAS & PARRY  
26 West 61st Street  
New York, NY 10023  
(212) 708-1890